IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF MARYLAND

John K. Wiebe, et al. Plaintiff, v. National Security Agency, et al. Defendants	Civil No. 0011CV3245 Judge Richard D. Bennett

DECLARATION OF STEVEN T.[1],
SID DEPUTY CHIEF OF STAFF FOR SIGINT POLICY
AND CORPORATE ISSUES, NATIONAL SECURITY AGENCY

I, Steven T., do hereby state and declare as follows:

Introduction and Summary

1. I am the Deputy Chief of Staff for SIGINT Policy and Corporate Issues for the Signals Intelligence Directorate (SID) of the National Security Agency (NSA), an intelligence agency within the Department of Defense. I am responsible for, among other things, protecting NSA Signals Intelligence (SIGINT) activities, sources, and methods against unauthorized disclosures. Under Executive Order No. 12333, 46 Fed. Reg. 59941 (1981), as amended on January 23, 2003, 68 Fed. Reg. 4075 (2003), and August 27, 2004, 69 Fed. Reg. 53593 (2004), and August 4, 2008, 73 Fed. Reg. 45325, SID is responsible for the collection, processing, and dissemination of SIGINT information for the foreign intelligence purposes of the United States. I have been

[1] Section 6 of the National Security Agency Act of 1959, 50 U.S.C. §402 note (Pub. L. No. 86-36) authorizes the National Security Agency to protect from public disclosure, among other categories of information, the names of its employees. Thus, the names of NSA employees will be referred to by first name, last initial. The Agency will provide the full name of any employee should the Court so require.

designated an original TOP SECRET classification authority under Executive Order (E.O.) 13,526, 75 Fed. Reg. 707 (Jan. 5, 2010), and Department of Defense Directive No. 5200.1-R, Information Security Program Regulation, 32 C.F.R. 159a.12 (2000).

2. My statements herein are based upon my personal knowledge of SIGINT collection and NSA operations, a review of the NSA information at issue, the information available to me in my capacity as the Deputy Chief of Staff for SID, and the advice of counsel.

3. In order to provide the necessary context for the discussion that follows, I will first describe NSA's origin and mission. The NSA was established by Presidential Directive in 1952 as a separately organized agency within the Department of Defense under the direction, authority, and control of the Secretary of Defense. NSA's foreign intelligence mission includes the responsibility to collect, process, analyze, produce, and disseminate SIGINT information for (a) national foreign intelligence purposes, (b) counterintelligence purposes, and (c) the support of military operations (*See* E.O. 12333, section 1.7 (c), as amended.

4. In performing its SIGINT mission, NSA exploits foreign electromagnetic signals to obtain intelligence information necessary to the national defense, national security, or the conduct of foreign affairs. NSA has developed a sophisticated worldwide SIGINT collection network that acquires, among other things, foreign and international electronic communications. The technological infrastructure that supports the NSA's foreign intelligence information collection network has taken years to develop at a cost of billions of dollars and untold human effort. It relies on sophisticated collection and processing technology.

5. In order to allow NSA to successfully perform its SIGINT mission, its activities must be done in secrecy. Original classification is the initial determination that NSA information requires, in the interest of national security, protection against unauthorized disclosure. There

are three levels of classification that are based on the damage to national security that could be expected if the information were subject to unauthorized disclosure.

a. "TOP SECRET" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security;

b. "SECRET" shall be applied to information, the authorized disclosure of which reasonably could be expected to cause serious damage to the national security; and

c. "CONFIDENTIAL" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.

6. In addition to classification, NSA information may also be Sensitive Compartmented Information (SCI), which is "information that not only is classified for national security reasons as Top Secret, Secret, or Confidential, but also is subject to special access and handling requirements because it involves or derives from particularly sensitive intelligence sources and methods." 28 C.F.R. § 17.18(a). Because of the exceptional sensitivity and vulnerability of such information, these safeguards and access requirements exceed the access standards that are normally required for information of the same classification level. Specifically, this declaration references special intelligence (SI) also known as Communications Intelligence (COMINT), which is a subcategory of SCI. SI identifies SCI that was derived from exploiting cryptographic systems or other protected sources by applying methods or techniques, or from intercepted foreign communications.

7. As a TOP SECRET original classification authority pursuant to section 1.3 of Executive Order (E.O.) 13526 dated December 29, 2009 (75 Fed. Reg. 707) it is one of my responsibilities to confirm the classification of NSA SIGINT information and/or information impacting NSA equities. Through the exercise of my official duties, I have become familiar with

the current litigation arising out of a request by the plaintiffs for the return of their personal computers/hard disk drives (HDD), portable media, and hard copy documents that I have been informed were seized by the Federal Bureau of Investigation (FBI). I am aware that a forensic analysis has been conducted by Tony T., Special Agent, Associate Directorate for Security and Counterintelligence, NSA, on the content of the HDDs and portable media.

8. It is my understanding that following his forensic analysis, to include a key word search of each of the HDD's, Tony T. created a "document[2]" containing the results of the search for each HDD. I have reviewed each of the eleven (11) documents listed in the chart below, and based on my authority as a TOP SECRET classification authority have determined that each document contains information that is currently and properly classified, as reflected in the chart below, in accordance with E.O. 13526, and protected from release by statutes, specifically Section 6 of the National Security Agency Act of 1959, 50 U.S.C. §402 note (Pub. L. No. 86-36); 18 U.S.C. §798; and Section 102A(i)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004, 30 U.S.C. §403-1(i)(1).

Item #	Description of Image	Plaintiff	Classification of Document
1	QWF2651B	Wiebe	TOP SECRET//SI
2	QWF26_52	Wiebe	TOP SECRET//SI
3	LL	Binney	TOP SECRET//SI
4	XXX	Loomis	TOP SECRET//SI
5	QHQ3	Drake	TOP SECRET//SI
6	QHQ4	Drake	TOP SECRET//SI
7	QHQ8_1	Drake	SECRET
8	QHQ10	Drake	SECRET
9	QHQ13	Drake	TOP SECRET//SI
10	QHQ14_1	Drake	TOP SECRET//SI
11	IBM VC009393	Drake	U//FOUO[3]

[2] The information provided to me was identified by plaintiff and image name. Although described as a "document," some of the information I reviewed was an email, email attachment or a series of paragraphs that appear to be part of a longer paper or essay.
[3] Information on this HDD is protected from release pursuant to the National Security Agency Act of 1959.

9. Each HDD referenced above is an Information System (IS) (i.e., any telecommunications and/or computer-related equipment) and must be protected at the classification level of the information stored on the IS. For instance, if TOP SECRET information is introduced to an UNCLASSIFIED IS, the IS must be considered TOP SECRET. Similarly, Information Storage Media (ISM) (e.g., diskettes, CD/DVD ROM discs) must be protected at the classification level of the information stored on the media, or the classification of the most restrictive data that can be accessed on the IS security domain in which the ISM has been used. (NSA Policy 6-22, "Label, Declassification, and Release of NSA/CSS Information Storage Media.) Therefore, each HDD is classified at the level indicated in the column on the far right of the above referenced chart.

10. It is my understanding that the FBI seized various documents/papers/Rolodex and index cards from plaintiffs Binney and Drake. Due to the volume of material seized, and pending the Court's rulings on certain legal issues, I have not conducted a full classification review of each and every piece of paper but can confirm the following:

Plaintiff	**Information Protected by the NSA Act of 1959**[4]	**Classified Information**	**OGA Equity**[5]
Binney	14 pages	39 pages	31
Drake	4510 pages	16 pages	0

11. I have been informed that the FBI seized a number of diskettes from the residence of plaintiff Drake. I have reviewed material printed from each, and confirm that each contains information protected by the National Security Agency Act of 1959.

[4] The National Security Agency Act of 1959 protects from disclosure any information related to the organization or function of the Agency, to include information with respect to the activities thereof, or the names, title, salaries or number of persons. The pages referenced in this column include this type of information, as well as the possibility of classified information.

[5] Some of the information presented to me for review clearly originated from another federal Agency or Department and is referred to herein as an "OGA" (other government agency). The NSA does not have the authority to agree to the release of this information absent the consent of the originator. I have been informed by the originator that this information has not been released to the general public.

Brand of Diskette	Document Title
Universal	• Drake_SID_change
Memorex	• Comms Plan 7 May 2002.doc • Comms.contract • Basis_comms Plan 7 May 2002
Sony	• [Locaton]_Report.txt • JAVATIME_drake_sqo_report.ppt

12. I have been informed that the FBI seized a number of disks/CD ROMS from the residence of plaintiff Binney. I have reviewed material printed from seven (7), and confirm that one contains TOP SECRET//SI information, one contains information protected by the National Security Agency Act of 1959, and one contains OGA information.

	Description of Media	Document Title
1	TDK IBM Floppy C3H15F2F2E2	[Title redacted] TOP SECRET//SI
2	Memorex CDRW S/N 0606051422954134	Contact List.csv, NSA Act of 1959
3	Memorex CDR 6143FI15191113LHA3	Info Superiority - Alberts & Garstka Dec 1999.ppt; OGA equity

13. All of the classified information described herein must be maintained in a facility designed to store classified information until such time as it is destroyed, in accordance with Executive Order 13526, NSA Policy 1-30, "Review of NSA/CSS Information for Public Dissemination," and Intelligence Community Directive Number 705, "Sensitive Compartmented Information Facilities."

14. In addition, the information described as protected by the National Security Agency Act of 1959 must be maintained in accordance with Agency regulations for the storage of protected information, until such time as the Agency agrees that it may be disclosed publically or is destroyed.

15. Pursuant to the National Security Agency Act of 1959, as well as other authorities, NSA has the right to protect from disclosure classified as well as certain other categories of protected information. The intentional public release of properly classified information is in violation of federal criminal law.

16. There are four statutory/policy based procedures to request the release of Agency information, which include the following: a Freedom of Information Act (FOIA) request (5 USC §552), a Mandatory Declassification Request (MDR) (based on E.O. 13526), a Privacy Act (PA) Request (5 USC §552a), or a request through the Agency's Prepublication Review office (Agency Policy 1-30). Current and former Agency employees are required to submit a pre-publication request whenever disclosing official NSA/CSS information intended for publication, to include references to work responsibilities and/or job descriptions on resumes.

17. I have caused a check to be conducted in the Agency offices that would routinely respond to FOIA, MDR, PA and pre-publication requests, and none of the plaintiffs, except plaintiff Loomis have submitted a request for any of the classified information found in their residences. Mr. Loomis has a pending pre-publication request for a book that is currently being processed by the Agency.

18. Each NSA employee is required to sign a Security Agreement upon hiring and an Access Termination Agreement upon retirement or resignation. These documents impose upon each employee three lifetime obligations to (1) safeguard all protected information; (2) submit all information intended for publication and/or public dissemination for classification and prepublication review; and (3) to report any unauthorized disclosures of protected information. I have been advised that each of the plaintiffs have executed a Security Agreement.

I declare under penalty of perjury that the foregoing is true and correct.

DATE: May 11, 2012

Steven T.
Deputy Chief of Staff for
SIGINT Policy and Corporate Issues,
Signals Intelligence Directorate